

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-243395  
(P2001-243395A)

(43) 公開日 平成13年9月7日 (2001.9.7)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード* (参考)
G 0 6 F 19/00		G 0 7 C 13/00	B 3 E 0 3 8
G 0 7 C 13/00		G 0 6 F 15/28	B 5 B 0 4 9

審査請求 未請求 請求項の数 7 O L (全 8 頁)

(21) 出願番号 特願2000-50779 (P2000-50779)

(22) 出願日 平成12年2月28日 (2000.2.28)

特許法第30条第1項適用申請有り 2000年1月11日 J  
apan Cyber Security Insti  
tute発行の「CYBER SECURITY MA  
GAZINE Vol. 2」に発表

(71) 出願人 000102739  
エヌ・ティ・ティ・アドバンステクノロジー  
株式会社  
東京都新宿区西新宿二丁目1番1号

(71) 出願人 500015272  
情報処理振興事業協会  
東京都文京区本駒込二丁目28番8号

(72) 発明者 白石 旭  
東京都新宿区西新宿二丁目1番1号 エ  
ヌ・ティ・ティ・アドバンステクノロジー株  
式会社内

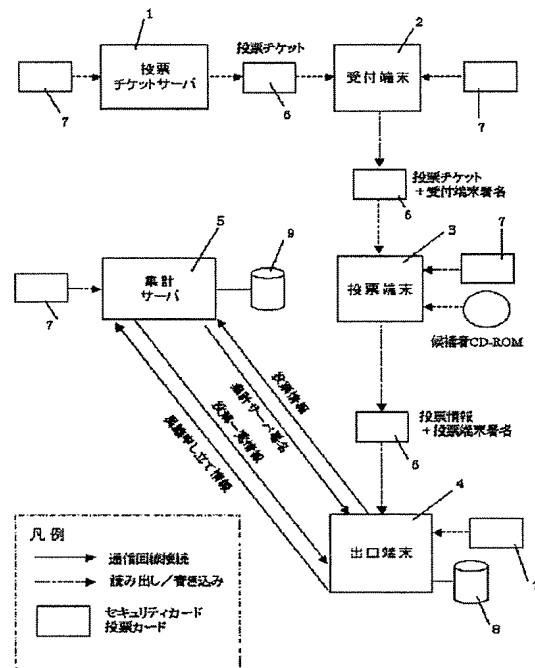
最終頁に続く

(54) 【発明の名称】 投票所方式による電子投票システム

(57) 【要約】

【課題】 本発明は、現行の選挙に適用でき、また、選挙に関する基本的な要求条件である、不正競争の防止、無記名性の保証、公平性の保証、削除／改ざん／水増しの防止、を満たす電子投票システムを提供することを目的とする。

【解決手段】 本発明による投票所方式による電子投票システムは、投票日の前に、投票チケットを格納した投票カードを有権者分作成する投票チケットサーバと、選挙人名簿との照合による投票者本人の確認をした後、投票チケットに対する受付端末署名を生成して投票カードに格納する受付端末と、投票者に候補者の氏名等を表示して投票を促し、投票行為によって得られた投票情報を投票カードに格納する投票端末と、投票カードから投票情報を読み出し、投票情報をオンラインで集計サーバへ送信する出口端末と、各投票所の出口端末から投票の都度送付される投票情報を受信し、投票時間終了後投票情報を集計して各候補者の得票数を出力する集計サーバから構成されることを特徴とする。



## 【特許請求の範囲】

【請求項1】 投票日の前までに投票チケットを格納した投票カードを有権者分作成する投票チケットサーバと、選挙人名簿との照合による投票者本人の確認をしたことに基ついて、上記投票チケットに対する受付端末署名を生成して上記投票カードに格納する受付端末と、上記投票カードから上記受付端末署名を読み出して検証し、投票者に候補者の氏名等を端末画面上に表示して投票を促し、投票行為によって得られた投票情報および上記投票情報に対する投票端末署名を上記投票カードに格納する投票端末と、上記投票カードから上記投票情報および上記投票端末署名を読み出し、上記投票端末署名を検証し、上記投票情報をオンラインで集計サーバへ送信し、また、上記集計サーバに送付した上記投票情報と、上記集計サーバから送付された集計サーバ署名を第一のデータベースに格納する出口端末と、各投票所の上記出口端末から投票の都度送付される上記投票情報を受信して第二のデータベースに格納し、上記集計サーバ署名を上記出口端末に送信し、投票時間終了後上記第二のデータベース上の上記投票情報を集計して各候補者の得票数を出力する上記集計サーバから構成されることを特徴とする投票所方式による電子投票システム。

【請求項2】 上記投票チケットが、暗号化されたシークエンス番号と投票チケットサーバ署名とから構成されることを特徴とする請求項1記載の投票所方式による電子投票システム。

【請求項3】 上記投票端末が、上記投票情報を識別するための情報として使用する第一の乱数を生成することを特徴とする請求項1記載の投票所方式による電子投票システム。

【請求項4】 上記出口端末では、第二の乱数を生成してセッション鍵を作り、上記セッション鍵を用いて上記投票情報を暗号化し、暗号鍵を用いて上記セッション鍵を暗号化して、暗号化された上記投票情報とともに上記集計サーバへ送信し、上記集計サーバでは、復号鍵を用いて上記セッション鍵を復号し、復号された上記セッション鍵を用いて上記投票情報を復号することを特徴とする請求項1記載の投票所方式による電子投票システム。

【請求項5】 上記セッション鍵の暗号化および復号に共通鍵方式を採用する場合に、上記共通鍵を安全に保管するセキュリティカードを用いることを特徴とする請求項4記載の投票所方式による電子投票システム。

【請求項6】 上記出口端末では、上記投票情報に対する出口端末署名を生成して、上記投票情報とともに上記集計サーバへ送信し、上記集計サーバでは、受信した上記出口端末署名を検証することを特徴とする請求項1、4又は5記載の投票所方式による電子投票システム。

【請求項7】 上記出口端末は、上記集計サーバが公開した投票一覧情報に対して、上記第一のデータベースを用いて上記集計サーバに送信した投票情報の削除、改ざ

ん、または投票の水増しをチェックし、もしそれらを検出した場合には、上記集計サーバへ異議申し立てを行うことを特徴とする請求項1、4、5又は6記載の投票所方式による電子投票システム。

【発明の詳細な説明】

【発明の属する技術分野】

【0001】本発明は、電子投票システムに関する。

【0002】

【従来の技術】電子投票は、セキュリティ技術の観点から各種の研究が行われているが、システムとして開発されているものは、オフライン形態の電子投票である。本発明のような、セキュリティ対策を反映したオンラインによるシステム開発は、現在のところ他には見られない。

【0003】ところで、電子投票システムを現行の選挙に適用した場合、投票情報をオンラインで集めて、開票をコンピュータで処理できるため、現行選挙での投票用紙の輸送や手作業による集計を無くすことができ、開票稼働の削減および開票時間の大幅な短縮が可能である。また、投票において端末画面上で候補者名を選択できるため、現行選挙で発生し易い誤記や判読不能等による無効票が無くすることができる。

【0004】電子投票システムを実現する方式は、

(A) ネットワーク方式・・・有権者は家庭等のPCからネットワークを通して投票を行う

(B) 投票所方式・・・有権者は投票所へ出向き、投票所に設置された投票端末で投票を行う  
の二つに大別できる。

【0005】上記のネットワーク方式では、見えざる所での買収や脅迫等が可能であり、公職選挙法としてネットワーク方式が受け入れられるまでには、本人の意思を確認する方法など多くの課題を解決しなければならない。一方、投票所方式では、投票管理者や立会人の監視の下で投票が行われるため、買収や脅迫等を防止できる。(少なくとも、無記名性を保証することにより、買収または脅迫された人が指示された候補者に投票したことを買収者や脅迫者に証明することができない。)そこで、投票の電子化には公職選挙法の改正が必須であるが、本発明では、法改正が実現され易いことを前提として、投票所方式を採用することとした。

【0006】

【発明が解決しようとする課題】本発明は、現行の選挙に適用できる電子投票システムを提供することを目的とする。

【0007】また、選挙に関する基本的な要求条件である、不正投票の防止、無記名性の保証、公平性の保証、削除/改ざん/水増しの防止、を満たす電子投票システムを提供することを目的とする。

【0008】また、投票情報をオンラインで集めて、開票をコンピュータで処理することにより、現行選挙での

10

20

30

40

50

投票用紙の輸送や手作業による集計を無くし、開票稼働の削減および開票時間の大幅な短縮を可能とすること、また、投票は端末画面上で候補者名を選択できるようにし、現行選挙で発生し易い誤記や判読不能等による無効票を無くすることを目的とする。

【0009】

【課題を解決するための手段】上記課題を解決するために、本発明による投票所方式による電子投票システムは、投票日の前までに投票チケットを格納した投票カードを有権者分作成する投票チケットサーバと、選挙人名簿との照合による投票者本人の確認をしたことに基づいて、上記投票チケットに対する受付端末署名を生成して上記投票カードに格納する受付端末と、上記投票カードから上記受付端末署名を読み出して検証し、投票者に候補者の氏名等を端末画面上に表示して投票を促し、投票行為によって得られた投票情報および上記投票情報に対する投票端末署名を上記投票カードに格納する投票端末と、上記投票カードから上記投票情報および上記投票端末署名を読み出し、上記投票端末署名を検証し、上記投票情報をオンラインで集計サーバへ送信し、また、上記集計サーバに送付した上記投票情報と、上記集計サーバから送付された集計サーバ署名を第一のデータベースに格納する出口端末と、各投票所の上記出口端末から投票の都度送付される上記投票情報を受信して第二のデータベースに格納し、上記集計サーバ署名を上記出口端末に送信し、投票時間終了後上記第二のデータベース上の上記投票情報を集計して各候補者の得票数を出力する上記集計サーバから構成されることを特徴とすることを特徴とする。

【0010】これにより、現行の選挙に適用できる電子投票システムを提供できる。

【0011】なお、投票チケットサーバ、受付端末、投票端末、出口端末、集計サーバは、単数でも複数でもよい。また、請求項1の「投票日の前」は、不在者投票の場合は告知日の前を意味する。

【0012】また、上記投票チケットが、暗号化されたシーケンス番号と投票チケットサーバ署名とから構成されることを特徴とする。これにより投票カードの偽造を防止するとともに投票情報の厳密な識別もできる（投票情報をシーケンス番号に対応させて管理する）。

【0013】また、上記投票端末が、上記投票情報を識別するための情報として使用する第一の乱数を生成することを特徴とする。これにより無記名性を損なうことなく不正投票を防止できる。

【0014】また、上記出口端末では、第二の乱数を生成してセッション鍵を作り、上記セッション鍵を用いて上記投票情報を暗号化し、暗号鍵を用いて上記セッション鍵を暗号化して、暗号化された上記投票情報とともに上記集計サーバへ送信し、上記集計サーバでは、復号鍵を用いて上記セッション鍵を復号し、復号された上記セ

ッション鍵を用いて上記投票情報を復号することを特徴とする。

【0015】また、上記セッション鍵の暗号化および復号に上記出口端末と上記集計サーバの共通鍵を用いること、または上記セッション鍵の暗号化に集計サーバの公開鍵を用い、復号に集計サーバの秘密鍵を用いることができる。上記セッション鍵の暗号化および復号に共通鍵方式を採用する場合に、上記共通鍵を安全に保管するセキュリティカードを用いることを特徴とする。これにより選挙の公平性を保証できる。

【0016】また、上記出口端末では、上記投票情報に対する出口端末署名を生成して、上記投票情報とともに上記集計サーバへ送信し、上記集計サーバでは、受信した上記出口端末署名を検証することを特徴とする。これにより上記出口端末の認証および通信文の改ざん防止ができる。

【0017】また、上記出口端末は、上記集計サーバが公開した投票一覧情報に対して、上記第一のデータベースを用いて上記集計サーバに送信した投票情報の削除、改ざん、または投票の水増しをチェックし、もしそれらを検出した場合には、上記集計サーバへ異議申し立てを行うことを特徴とする。これにより票の削除/改ざん/水増しを防止できる。

【0018】

【発明の実施の形態】本発明による電子投票システムの構成を図1に示す。

【0019】図において、1は投票チケットサーバ、2は受付端末、3は投票端末、4は出口端末、5は集計サーバ、6は投票カード、7はセキュリティカード、8は第一のデータベース、9は第二のデータベースである。以下、電子投票システムの構成要素である投票チケットサーバ1、受付端末2、投票端末3、出口端末4、集計サーバ5について順次説明する。

【0020】(1)投票チケットサーバ

投票チケットサーバ1は、有権者数に応じて、選挙区に1台または複数台設置する。投票チケットサーバ1は、投票日の前（不在者投票等を考慮すると告示日の前）までに、投票チケットを格納した投票カード6（ICカードを使用できる）を有権者分作成する。投票カード6は、現行選挙における投票用紙に相当する。投票チケットは、チケットサーバ署名とシーケンス番号から構成される。選挙委員会等が交付した正当なものであることを証明し、投票カードの偽造を防止し、投票情報の厳密な識別を可能とするためである。

【0021】(2)受付端末

受付端末2は、投票所に1台設置する。受付端末2では、選挙人名簿との照合による投票者本人の確認をしたことに基づいて、投票チケットに対する受付端末署名を生成して投票カード6に格納する。受付端末署名は、この投票カード6は投票所受付にて投票管理者から交付さ

れたものであることを証明するものであり、またこれらの受付端末2の行為により、この投票カード6を持つ投票者は投票の資格を持ちかつ1回目の投票であることを保証する。

#### 【0022】(3) 投票端末

投票端末3は、投票所に複数台設置する。投票端末3は、投票カードに格納された受付端末署名を読み出して検証した後、投票者に候補者の氏名等を端末画面上に表示して投票を促し、投票行為によって得られた投票情報および投票情報に対する投票端末署名を投票カード6に格納する。投票者の投票操作は、老人や主婦などコンピュータに不慣れな人や体の不自由な人を考慮して、タッチパネルを用いた画面上の指による選択など簡易なものとする。また、例えば衆議院議員選挙において、小選挙区選出議員は投票したいが、比例代表選出議員は棄権したい場合等を考慮して、投票の選択肢として、候補者名に加えて「白票」を設ける。さらに、候補者選択における誤操作の可能性を考慮し、選択された候補者に対する確認画面を表示し、誤操作の訂正を可能とする。

#### 【0023】(4) 出口端末

出口端末4は、投票所に1台設置する。出口端末4は、投票カード6から投票情報および投票端末署名を読み出し、投票端末署名を検証した後、投票情報をオンラインで集計サーバ5へ送信する。出口端末4と集計サーバ5との間の通信文は暗号化してネットワーク上の盗聴を防ぐとともに、通信文に対する出口端末4の署名を添付することにより、出口端末4の認証および通信文の改ざん防止を可能にする。なお、出口端末4では、集計サーバ5に送付した投票情報と、集計サーバ5から送付された集計サーバ署名を第一のデータベース8に格納する。その際に出口端末4近傍で投票カード6を回収する。回収した投票カード6は、後日の開票結果に対する異議申し立て訴訟のための証拠保全の観点から、密封して保管する。

#### 【0024】(5) 集計サーバ

集計サーバ5は、選挙区に1台設置する。集計サーバ5は、各投票所の出口端末4から投票の都度送付される投票情報を受信して第二のデータベース9に格納し、集計サーバ署名を出口端末4に送信する。また、投票時間終了後第二のデータベース9上の投票情報を集計して各候補者の得票数を出力する。

【0025】なお、各構成要素の機能概要を表1にまとめて示す。また、セキュリティカード7は、投票情報の暗号及び署名に使用する鍵の秘密漏洩防止等のため、上記全ての投票チケットサーバ1、受付端末2、投票端末3、出口端末4、集計サーバ5に使用される。

【0026】(選挙に対して要求される条件を満たす方式) 選挙に対する基本的な要求条件は、藤崎・太田・岡本「投票所を仮定した実用的な電子投票方式」、信学技報、ISEC93-24、1993に記載されており、

次のようである。

(1) 不正投票の防止：有権者が一回のみ投票ができること。

(2) 無記名性の保証：誰が誰に投票したかは秘密であること。

(3) 公平性の保証：投票が終了するまで、何人たりとも投票の途中経過を知ることができないこと。

(4) 削除/改ざん/水増しの防止：投票者によって投票された投票結果が、削除、改ざん、水増しされないこと。

【0027】上記要求条件を表2にまとめて示す。

【0028】以下に、上記各々の要求条件に対する本電子投票システムでの実現方式を順次説明する。なお、この検討に当たっては、下記事項(A)～(D)を前提とする。

(A) 投票者はプライバシー保護上、投票行為が誰からも監視されないため、不正を行い易い。

(B) 投票所の選挙管理者は、立会人や投票者の監視下にあるので、不正は行えない。

(C) 集計サーバの選挙管理者は、立会人の監視下にあるので不正は行えないが、投票者にはその状況が見えないため、不信感を抱かせる懸念がある。

(D) ソフトウェア等、電子投票システム自体は、不正な動作をしない。

#### 【0029】(1) 不正投票の防止

投票しようとする人が、この投票所で投票をする資格があり、かつ1回目の投票であることの確認は、現行選挙と同様に、投票所受付にてハガキに印刷されて郵送された投票券の提示を求め、投票管理者がその投票所に割当てられた選挙人名簿に投票済みの印を記入することにより行う。

【0030】その後本電子投票システムでは、上記確認の終了した投票者に対して、投票管理者が受付端末2で受付端末署名を書き込んだ投票カード6を交付する。この受付端末署名は、投票端末2においてチェックされるため、事前に投票チケットをコピーするなどして偽造した投票カード6を投票所に持ち込んでも、受付端末署名が書き込まれていないために投票端末3で偽造が検出されるので、投票することはできない。

【0031】ただし、投票端末3で受付端末署名が無いことを検出した場合、投票カード6の不良やシステムの動作不良と偽造カードとの切り分けをその場で行うことは運用的に困難であることから、投票を行う権利を尊重して投票カード6を再交付せざるを得ない。このように、受付端末2で最初に正規に交付された投票カード6と、偽造カードの代わりに再交付された二枚目の正規の投票カード6を使用して、二重投票が行われる危険性がある。本システムでは、投票所の出口で投票管理者が投票者から一枚の投票カード6を受け取り、その投票カード6を出口端末4に挿入して投票情報を集計サーバ5へ

送信するので、二枚の投票カード6の使用による二重投票を防止することができる。

#### 【0032】(2) 無記名性の保証

無記名性を保証するために、投票カード6には投票者を特定できる情報を一切格納しない。

【0033】ただし、後述の削除/改ざん/水増しの防止を実現するためには、個々の投票情報を識別するための情報が必要である。これを無記名性を損なうことなく実現するために、投票端末4で生成した第一の乱数を、投票情報を識別するための情報として使用する。

【0034】選挙区の有権者数に対して第一の乱数の桁数を十分大きく取ることにより、同一選挙区内の複数の投票端末で同一の乱数が生成される確率は極めて小さくなる。しかし、一票の票の重みを考慮した場合、いかに確率が小さくても同一の乱数が生成されたことにより、ある投票情報が無効化されることは許されない。このため、投票チケットにシーケンス番号を包含し、このシーケンス番号を万が一第一の乱数が一致した投票情報を更に識別するための補助情報として使用する。

【0035】ただし、受付端末2の操作者が投票チケット内のシーケンス番号を見ることができると、投票者とシーケンス番号、シーケンス番号と投票情報のマッピングが可能となり、無記名性を損なう恐れがあるため、投票チケット内のシーケンス番号は暗号化して投票所受付の投票管理者には見えないようにし、投票端末3のみで復号する。

#### 【0036】(3) 公平性の保証

投票所内の受付端末2、投票端末3、出口端末4は投票管理者および立会人の監視下に置かれ、集計サーバ5は開票管理者および立会人の監視下に置かれている。したがって、投票時間中に投票の途中経過が外部に漏れる可能性があるのは、出口端末4と集計サーバ5との間の通信のみである。

【0037】出口端末4から集計サーバ5へ送信される投票情報の盗聴防止は以下により実現する。出口端末4では、第二の乱数を生成してセッション鍵を作り、このセッション鍵を用いて投票情報を暗号化する。さらに、暗号鍵を用いてセッション鍵を暗号化して、暗号化された投票情報とともに集計サーバ5へ送信し、集計サーバ5では、復号鍵を用いてセッション鍵を復号し、復号されたセッション鍵を用いて投票情報を復号する。また、セッション鍵の暗号化および復号に出口端末4と集計サーバ5の共通鍵を用いること、またはセッション鍵の暗号化に集計サーバ5の公開鍵を用い、復号に集計サーバ5の秘密鍵を用いることができる。なお、出口端末4と集計サーバ5の共通鍵は、セキュリティカード7(ICカードを使用できる)内に安全に保管し、出口端末4および集計サーバ5の立ち上げ時に、インストールされる。

#### 【0038】(4) 削除/改ざん/水増しの防止

投票所内の受付端末2、投票端末3、出口端末4は投票者の目に届く範囲内にある。しかし、集計サーバ5は目の届かない場所に設置されるため、投票者は集計サーバ5の不正処理が心配となる。現行選挙では開票時の不正を監視するために立会人を置くとともに、それ以外の人の傍聴も可能である。本電子投票システムにおいても、立会人の監視の下で開票が行われることを前提としているが、集計サーバ5の処理内容に不正がないかを目で見て確認することはできない。このため、投票者が監視できる出口端末4で、集計サーバ5による投票情報の削除/改ざん/水増しを監視するメカニズムを実現する。

【0039】具体的には、出口端末4では、投票情報に対する出口端末署名を生成して、投票情報とともに集計サーバ5へ送信し、集計サーバ5では、受信した出口端末署名を検証する。また、出口端末4は、集計サーバ5が公開した投票一覧情報に対して、第一のデータベース8を用いて集計サーバ5に送信した投票情報の削除、改ざん、または投票の水増しをチェックし、もしそれらを検出した場合には、集計サーバ5へ異議申し立てを行う。

【0040】(現行選挙との親和性) 本電子投票システムでは、現行選挙の電子化へのスムーズな移行を目標に、現行選挙における種々の制度項目への対応を検討した。以下、順次説明する。

#### 【0041】(1) 複数同時選挙

衆議院議員選挙および参議院議員選挙における小選挙区と比例代表、地方公共団体選挙における首長選挙と議会議員選挙あるいは県会議員選挙と市会議員選挙、更には、衆議院議員選挙と同時にされる最高裁判事国民審査など、同一の投票日に複数の選挙の投票を実施する機会が多い。現行選挙においては、投票用紙の交付、投票の記載、および投票の投函を、選挙の数だけ繰り返している。

【0042】本電子投票システムにおいては、投票者の利便性を考慮して、一枚の投票カード6を用いて、一箇所の投票端末3で、複数の選挙に対する投票を可能とする。これを実現するための主要事項を以下に示す。

(A) 一枚の投票カードに格納される一つの投票チケットを、同日に実施される個々の選挙ではなく、同日に実施される複数の選挙全体に対応させる。

(B) 投票端末では、投票種別に対応した候補者情報を表示し、投票を受け付ける。候補者の表示と投票の行為を、同日に実施される全ての選挙に対して繰り返し、全ての投票情報を一枚の投票カードに格納する。また、最高裁判事国民審査等のように、一つの選挙に対して複数の氏名の選択を可能とする。

(C) 集計サーバでは、上記全ての投票情報を第二のデータベース9に格納し、開票時には、各選挙別の候補者毎に得票数を集計する。

#### 【0043】(2) 投票記載手段

現行選挙においては、投票用紙に候補者の氏名を自書（手書き、地方公共団体選挙においては記号式投票も可能）することが定められているが、点字投票および代理投票も認められている。

【0044】本電子投票システムにおいては、公職選挙法の改正を前提として、投票端末の画面に候補者の氏名等を表示し、投票したい候補者の氏名をパネルタッチで選択することにより、投票用紙に候補者の氏名を自書する代わりとする。また、現行選挙における補助者が投票者の指示する候補者氏名を投票用紙に記載する代わりに、補助者が投票者の指示する候補者氏名をパネルタッチすることにより、代理投票を可能とする。なお、投票用紙への自書がパネルタッチによって簡略化されることにより、電子投票では代理投票の要求が減少すると考えられる。しかし、本電子投票システムで使用予定のタッチパネルでは点字の表示ができないため、点字投票は本システムの対象外とせざるを得ない。将来的に投票専用端末を開発する場合には、点字投票への対応が一つの検討課題となる。

#### 【0045】(3) 不在者投票

不在者投票は名簿登録或は仕事先等の市町村選挙管理委員会での投票、指定病院等の指定施設での投票、郵便での投票が認められている。不在者投票に対しては、下記のいずれかの方法で対応可能である。

(A) 不在者投票を行う場所に、受付端末2と投票端末3と出口端末4を設置し、通常の投票と同様に投票情報を集計サーバ5の第二のデータベース9に保管する。

(B) 不在者投票を行う場所に、受付端末2と投票端末3を設置し、投票情報が格納された投票カードを不在者投票用封筒に入れて保管し、投票日に不在者投票用の出口端末を用いて、投票カード6内の投票情報を集計サーバ5へ送信する。ただし、郵便による不在者投票は本システムで対応できない。

#### 【0046】(4) 在外投票

上記不在者投票と同じ対応であり、郵便投票以外は本システムで対応可能である。

(A) 不在者投票を行う場所に、受付端末2と投票端末3と出口端末4を設置し、通常の投票と同様に投票情報

を集計サーバ5の第二のデータベース9に保管する。

(B) 不在者投票を行う場所に、受付端末2と投票端末3を設置し、投票情報が格納された投票カードを不在者投票用封筒に入れて保管し、投票日に不在者投票用の出口端末を用いて、投票カード6内の投票情報を集計サーバ5へ送信する。

【0047】なお、本電子投票システムにおける現行選挙制度への対応の範囲を表3にまとめて示す。

#### 【0048】

- 10 【発明の効果】以上説明したように、本発明によれば、現行の選挙に適用できる電子投票システムを提供できる。

【0049】また、選挙に関する基本的な要求条件である、不正投票の防止、無記名性の保証、公平性の保証、削除/改ざん/水増しの防止、を満たす電子投票システムを提供できる。

- 20 【0050】また、本電子投票システムを現行の選挙に適用することにより、投票情報をオンラインで集めて、開票をコンピュータで処理できるため、現行選挙での投票用紙の輸送や手作業による集計が無くなり、開票稼働の削減および開票時間の大幅な短縮が可能となる。また、投票は端末画面上で候補者名を選択できるため、現行選挙で発生し易い誤記や判読不能等による無効票が無くなる効果も期待できる。

#### 【図面の簡単な説明】

【図1】本発明による電子投票システムの構成を示す図である。

#### 【符号の説明】

- 1 投票チケットサーバ  
2 受付端末  
3 投票端末  
4 出口端末  
5 集計サーバ  
6 投票カード  
7 セキュリティカード  
8 第一のデータベース  
9 第二のデータベース

【表1】

機能概要		
構成要素	設置台数	機能概要
投票チケットサーバ	1～数台／選挙区	投票チケットを生成し、投票カードに書き込む。
受付端末	1台／投票所	受付端末署名を生成し、投票カードに書き込む。
投票端末	数台／投票所	候補者情報を表示し、投票を促す。
出口端末	1台／投票所	投票情報と投票端末署名を投票カードに書き込む。
集計サーバ	1台／選挙区	投票情報を集計サーバへ送信するとともに、投票情報と集計サーバから送信された集計サーバ署名をデータベースに格納する。(投票時) 集計サーバが公開した投票一覧情報とデータベースの内容との突き合わせチェックを行い、不正検出時集計サーバへ異議申し立て情報を送信する。(開票時) 出口端末から送信された投票情報をデータベースに格納し、集計サーバ署名を出口端末に送信する。(投票時) データベース上の投票内容を集計し、候補者毎の得票数を出力する。(開票時)

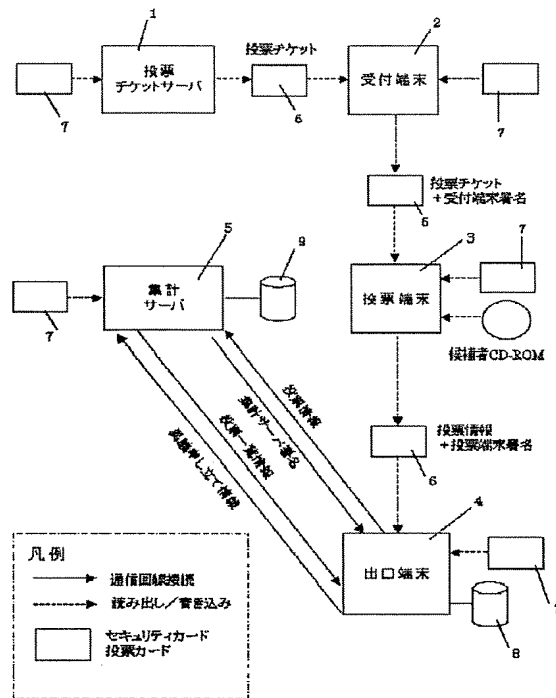
【表2】

選挙の要求条件	
要求条件	内容
不正投票の防止	有権者が一回のみ投票ができること。
無記名性の保証	誰が誰に投票したかは秘密であること。
公平性の保証	投票が終了するまで、何人たりとも投票の途中経過を知ることができないこと。
削除/改ざん/水増しの防止	投票者によって投票された投票結果が、削除、改ざん、水増しされないこと。

【表3】

電子投票システムにおける現行選挙制度への対応の範囲			
現行の選挙制度項目		対応内容	記事
投票種別	衆議院議員選挙	<ul style="list-style-type: none"> <li>1枚の投票カード(投票チケット)で複数選挙に対する投票を可能とする</li> <li>投票端末で投票種別に対応した候補者情報を表示し、投票を受け付ける</li> <li>集計サーバで投票種別に対応した投票情報のデータベース化および集計処理を行う</li> </ul>	小選挙区/比例代表/最高級科事国民審査
	参議院議員選挙		小選挙区/比例代表
	地方選挙		首長/議会議員
投票記載手段	手書き	画面上に表示した候補者をパネルタッチで選択する	公職選挙法改正が必要
	点字	システム対応外とする	将来的に点字端末の開発が必要
	代理	立会人の監視の下で代理人が端末を操作する	現行運用と同じ
不在者投票	名簿登録の市町村選挙管理委員会	<ul style="list-style-type: none"> <li>受付端末/投票端末/出口端末を不在者投票所に設置して実施する</li> <li>投票情報は、開票作業時まで出口端末/集計サーバのデータベースに保存する</li> </ul>	本研究開発ではローカル LAN を使用
	仕事先等の市町村選挙管理委員会		
	指定病院等の指定施設		
在外投票	郵便	システム対応外とする	
	在外公館投票	<ul style="list-style-type: none"> <li>受付端末/投票端末/出口端末を不在者投票所に設置して実施する</li> <li>投票情報は、開票作業時まで出口端末/集計サーバのデータベースに保存する</li> </ul>	本研究開発ではローカル LAN を使用
	郵便投票	システム対応外とする	
	帰国投票	不在者投票と同じ	

【図1】



フロントページの続き

(72)発明者 田中 利清  
東京都新宿区西新宿二丁目1番1号 エ  
ヌ・ティ・ティ・アドバンステクノロジー株  
式会社内

Fターム(参考) 3E038 AA01 GA02 KA03  
5B049 AA05 AA06 BB39 DD01 EE02  
FF09 GG10